EXHIBIT B5

Jira Compliance, Part 1: Approvals and Segregation of Duties

When configuring an enterprise application ecosystem, compliance has to be considered. State, federal, and international regulations will inevitably intersect with nearly every business at some point. And the results of non-compliance can be costly and even damage the organization's reputation.

Here is a list of some of the most common compliance standards U.S. companies must consider:

- HIPAA
- SOX
- PCI DSS
- GLBA
- FISMA
- CCPA
- GDPR (if they have customers in the EU)

To maintain compliance with these, and more, companies need to monitor their data integrity and internal processes. Internal audits are a necessary part of the compliance process. This means that setting up the systems to support quick and efficient audits is also a smart consideration.

Why compliance can be difficult

c

Suddenly, instead of just working against an ever-evolving backlog of business requirements to deliver value to their customers, they are required to produce a large number of compliance artifacts, essentially defending the work that they have done in the past against external or internal auditors. This creates not only the feeling of inefficiency but also, unfortunately, hostility.

So there are a lot of negatives to becoming compliant without considering the impact of those requirements on the teams. Configuring your Atlassian tools (and indeed your whole Enterprise application ecosystem) in a way that supports those requirements will minimize the strain that compliance produces upon your teams. It will make life easier and will allow you to scale your organization to new heights while maintaining the same momentum in your teams.

And so, it becomes very critical to configure the Atlassian tools based on your compliance requirements.

Let's explore Jira Compliance

With so many enterprises relying on Atlassian Jira, it's important to know how to handle compliance tasks and optimize Jira for compliance. Jira Software and Jira Service Manager track changes, development work, and service requests like access to systems and employee off-boarding. We'll be covering four main aspects of compliance in Jira:

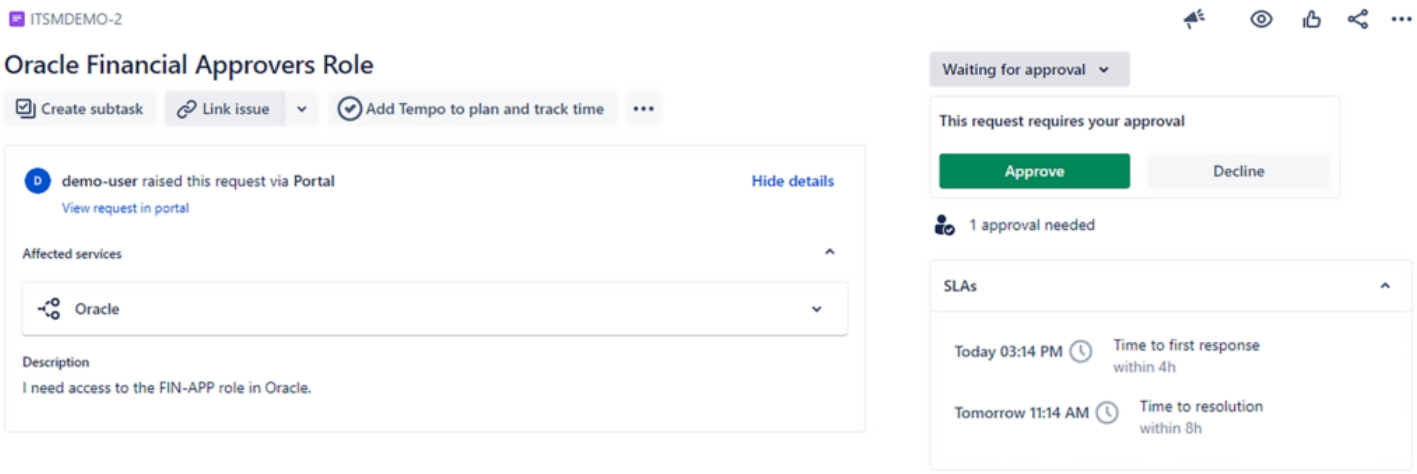
1. **Approvals** – ensuring changes to the system and/or data can only be made by those authorized to do so
2. **Segregation of Duties** – ensuring that no one person can implement a change on their own in Jira without the appropriate number of eyes looking at that work
3. **User Management** – maintaining appropriate user permissions and restrictions; knowing who was on-boarded and off-boarded, when, and all the systems that they gained access to in between
4. **Auditability** – the ability to quickly and easily obtain readable exportable reports about activity that took place in Jira

NOTE: Many of the points below touch on the principles of *logical separation*. Read our blog series on logical separation for a deeper dive.

Approvals in Jira

c

You can create multiple fields for different types of approvals, even within a single Jira workflow, and automatically configure the number or percentage of approvals required at that stage in the workflow. Additionally, JSM allows you to use Insight Asset Management to define your service catalog, and each item in that catalog can have its own unique approvers group.



This means that, when configured properly, a user can follow a simple process. For example:

1. Submit a Service Request for access to a particular system
2. Select the specific module and role for that Financial system within the services field in the appropriate request type
3. Click "Submit."

Once submitted, Jira will:

1. Automatically identify the appropriate approvers' group for that module and role
2. Notify those approvers via email or push notification

The request will not be able to proceed without those required approvals. And once the approvers have approved, the request can be configured to automatically route to the next appropriate status — perhaps, to an Oracle system administrator to grant access to the requestor based on the approved request.

All of these approvals are tracked in an auditable manner within Jira so that it is clear who received what role, when, and who approved the systems access.

If you don't have Jira Service Management, you can also utilize popular automation plugins like Power Scripts for Jira to implement similarly intuitive approval processes within native Jira Software workflows.

c

own.

For example, there may be a Senior Director who technically has the permission to approve a change in Jira. However, that Senior Director should not be able to create *and* approve his own change. Segregation of duties means that even though that person has the authority to approve other changes, they cannot approve their own change.

This same concept can be extended to apply to all sorts of activities. For example, the person who approved the change should not also be able to serve as the admin who administrates that change.

A lack of segregation of duties opens a company up to security vulnerabilities, audit failures, and poor processes in general. Without segregation of duties, someone could theoretically create, approve, and administrate their request to access data such as sensitive financial information or protected health information. So, configuring Jira to support segregation of duties is vital.

An example

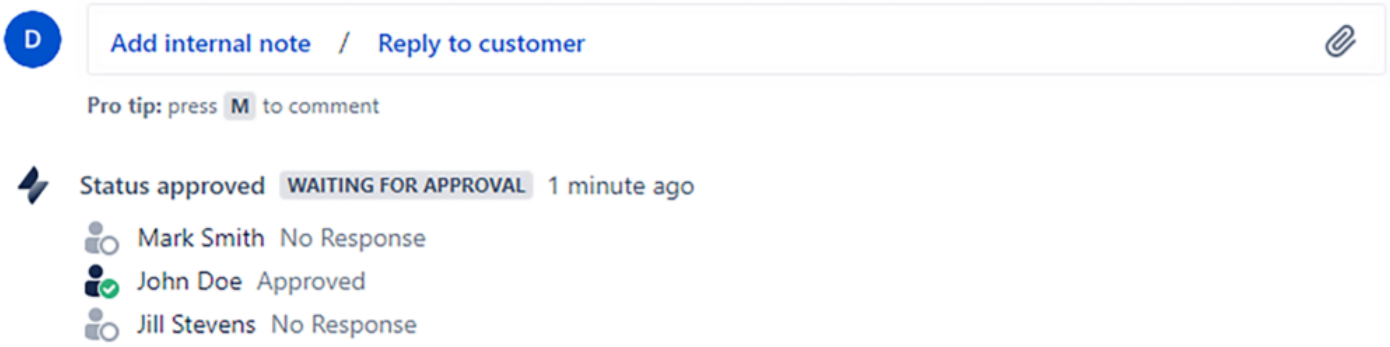
One useful way to implement segregation of duties policies in Jira is by using custom fields that record important roles for each ticket.

For example, the **requester** of a change, the **approver** of a change, the **administrator** of a change, and the **reviewer** of a change are all different roles. And ideally, those should not be the same person. So we need to capture the identity of the person serving in those roles with separate user picker fields.

The easiest way to do this is to create unique custom fields for each of those roles. They then need to associate them with the “Change“ Issue Type. And, finally, they need to automatically populate those fields as different users perform those activities.

For example, when a ticket enters the “Review” status, there may be ten different people who can potentially approve it. But the one person who approves that ticket would have their name automatically populated in the “Change Approved By” field. That way, if that person is also in the administrators’ group, the system can exclude them from the group with authority to approve that ticket, preventing the “Change Approved By” user from executing that transition.

c



This type of business logic allows companies to enforce segregation of duties in Jira workflows. It is also a requirement to maintain compliance with standards like SOX, PCI, and ITAR.

We will cover the second half of this topic in our next article, Compliance in Jira, User Management and Auditability .

To explore the wider topic of data security in the Atlassian ecosystem, download our whitepaper, "Your Quick Hit Guide to Atlassian Cloud Security."

Need help with your compliance journey?

Talk to an expert today

atlassian jira | compliance | JIRA

c

Clayton Chancey,
Solutions Architect

You may also be interested in:

Atlassian Integrations

Gitlab Integrations: Popular Synchronization to Simplify Software Development

GitLab integrations make collaboration more convenient and productive. Working on a project often requires the use of several tools and...

Read Blog

Atlassian

Jira Service Management Cloud: Standard vs Premium vs Enterprise

This article compares the three service tiers available for Jira Service Management on the Atlassian Cloud platform. If you're also...

How to Know if Your Jira-GitLab Integration is Successful

Read Blog

Atlassian Integrations

How to Know if Your Jira-GitLab Integration is Successful

In a previous article, we covered what organizations should consider when researching and implementing a Jira-GitLab integration. But the next...

c

Solutions Training

Resources About

Support

- Agile Solutions
- Product Solutions
- Cloud Solutions
- Atlassian Solutions
- Software Development

- Case Studies
- Webinars
- White Papers
- Blog

- Training Courses
- Certifications
- Team Training
- Ways to Learn

- Our Team
- Our Partners
- Cprime Careers
- Contact Us

Stay in touch with us